Department of Health Care Policy & Financing

THIRD PARTY USER ACCESS MODIFICATION / REVOCATION

This Modification/Revocation Request will be used to modify or terminate access to the systems the Department administers or maintains. This Request can only be used for those third party users who already have access to DOHCPF systems. "Revocation" means ALL system access privileges will be revoked. "Modification" means current system access privileges are to be modified – access to certain systems can be revoked, access to additional systems can be requested. The Request must be completed in full and signed by the User's Supervisor. **Manager must immediately notify the Department Information Security Administrator to terminate account access for any user no longer authorized to perform required obligations and responsibilities within the system.**

☐Addition ☐Modification ☐Revocation ☐Reactivation ☐Name Change ☐Other Change

Effective Date: _____
(If left blank, it is assumed to be immediate)

Reason for Addition/Modification/Name Change/Reactivation/Revocation/Change: _____

User First Name: _____ Middle Initial: _____ Last Name: _____

User Agency/Section: _____

User Address: _____

Work Number: _____ Email Address: _____

Last four digits of SSN: or any other 4 digit numeric identifier: _____
This information is used solely to verify User identity for resetting passwords.

Manager Name: _____ Telephone Extension: _____

System Access to be Modified or Revoked: (Please indicate which systems require access modification or revocation and current User IDs. If modification is being requested, please be specific as to what modification is necessary.)

☐ HCPF WEB PORTAL (Secured Sites) _____

☐ HCPF CBMS WEB PORTAL (HCPF State Workers, MA Sites, PE Sites and other CBMS HCPF Contractors)_____

☐ MMIS _____ ☐ MMIS-DSS _____

☐ COLD _____

☐ PDCS _____ (Prescription Drug Card System form also required)

☐ CBMS _____ ☐ CBMS-DSS _____
(CBMS Access form required if requesting new or additional access. Include current CBMS user role if additional access.)

☐ COFRS _____ (Financial System Access form required if requesting COFRS, FDW or Document Direct)

☐ ULTC BUS_____ County Code_____ Class (SEP, DDD, etc) _____ ☐Local User ☐ Administrator ☐Other _____

☐ SAVE: _____

☐ Other System (Please specify): _____

Manager Signature: _____ **Date:** _____

Agency Security Administrator Signature: _____ **Date:** _____

HCPF Contract/Program Manager Signature: _____ **Date:** _____

(By signing, Manager attests that information provided is accurate, all prior access no longer needed is revoked, and any additional access requested is necessary to perform User's authorized responsibilities.)

Department of Health Care Policy & Financing

(Sign Agreement Only If Requesting Additional, Modification, Change or Reactivation)

SYSTEM USER AGREEMENT

By signing this Agreement, you consent and agree to be bound by all of the terms and conditions below, and you understand that any failure to comply with the terms and conditions may result in sanction, which can include termination of your user account. This Agreement applies to any/all systems you are granted access to by the Department of Health Care Policy and Financing. Completion of this Agreement is required before access will be granted.

System users understand that the Colorado Department of Health Care Policy and Financing (Department) owns, either solely or jointly with another State agency, the system application and all information that can be accessed through the system. Access to the system is restricted to those who have been authorized by the Department and their Security Administrator (if any) to enter.

System users are responsible for reading and complying with any/all applicable Department Privacy/Security Policies and Procedures as provided by the Department.

System users shall only use/disclose records and/or information that is created, received, maintained, or transmitted within the system as authorized by the Department, and/or as required to perform authorized obligations and responsibilities.

System users shall limit use/disclosure of records and/or information concerning Colorado Medical Assistance Program clients or applicants to the purposes directly connected with the administration, operation, or oversight of the Colorado Medical Assistance Program.

System users shall not knowingly cause or allow the addition, modification, destruction or deletion of any records and/or information accessible through the system, except solely in the course of performing their authorized work.

System users shall not make unauthorized use/disclosure of, or knowingly permit unauthorized access by others to, records and/or information contained within the system.

System users shall maintain an assigned, unique User ID. Users understand that they are responsible for any activity that occurs under their individual User ID. In the event that a User suspects that another person knows and/or has used his/her User ID and Password, the User must notify his/her Security Administrator immediately. Additionally, it is a security violation for a User to mask his/her identity or assume the identity of another User.

System users shall practice adequate Password management by keeping Passwords confidential. Users shall not share their Passwords with anyone else for any reason, and are discouraged from writing down their Passwords and posting in view of others.

System users understand that the Department may monitor, track, and record all Users and uses of the system at any time. (This includes all Internet usage and email, when Department connection is utilized.)
System users shall not attempt to alter, exploit, or otherwise interfere with the system application. The State/Department has the right to update the system at any time.

System users shall report any violations, or suspected violations of this Agreement immediately to their Supervisor and/or Security Administrator.

System users understand that any violation of this Agreement may be cause for sanction including account termination.

System users who are also State employees shall not use state time, property, equipment, or supplies for private profit or gain, or for any other use not in the interest of the State of Colorado.

System users who are designated as Security Administrators also have the following responsibilities:

Authorized Security Administrators shall ensure system users are aware of any/all applicable Department Privacy/Security Policies and Procedures and any updates/clarifications provided by the Department.

Authorized Security Administrators shall establish additional appropriate administrative, technical, procedural, and physical safeguards to ensure the confidentiality, integrity, and availability of client/applicant records and/or information created, received, maintained, or transmitted within the system.

Authorized Security Administrators shall ensure all computers used to access the system contain appropriate, updated anti-virus software.

Authorized Security Administrators shall immediately notify the Department Security Administrator to terminate account access for any user no longer authorized to perform required obligations and responsibilities within the system.

Authorized Security Administrators shall serve as the Department's contact for any privacy/security issue that requires escalation or investigation.

Authorized Security Administrators shall immediately report alleged or actual privacy/security incidents to the Department Security Administrator. These would include any/all incidents that could affect the system such as virus incidents, unauthorized access, improper use/disclosure of client records and/or information, and any other activity that may be considered a violation, or suspected violation, of this Agreement.

The Department reserves the right to edit/update this Agreement at any time.

User Name (First, MI, Last): _____

User Signature: _____ Date: _____